Patent Claims

1. A random number generator (100), comprising:

- a true random number generator (101);
- a pseudo-random number generator (102), arranged to generate a pseudo-random sequence by using the true random numbers produced by said true random number generator (101) as random seed; and
- a mixing logic (103) connected between said true random number generator (101) and said pseudo-random number generator (102) and arranged to alter the behaviour of said pseudo-random number generator (102) by using the random seed,

characterised in that said true random generator (101) is arranged to generate a random sequence of bits having variable rate, and in that said mixing logic (103) comprises a generator (205, 206, 207) of an alteration signal (TC1) intended to change the behaviour of said pseudo-random number generator (102) at multiple random instants in the interval between two subsequent seeds, thereby obtaining in said interval multiple pseudo-random sequences of random lengths shorter than the random length determined by the arrival of two subsequent seeds, said generator (205, 206, 207) of the alteration signal being connected so as to receive said seed and generate said alteration signal (TC1) by processing said seed by means of the sequence generated by said pseudo-random number generator (102).

2. A random number generator (100) as claimed in claim 1, wherein said generator (205, 206, 207) of the alteration signal (TC1) comprises:

- a first down counter (205) arranged to count down from a first random number, represented by a first group of bits which are part of a randomly rotated version of a seed received by said alteration signal generator (205, 206, 207), said first counter (205) loading said first random number and starting its countdown whenever a seed is available and, between the occurrence of two subsequent seeds, whenever it generates a terminal count signal, said terminal count signal being fed to said pseudo-random number generator (102) as alteration signal (TC1);
- a second down counter (206), which is arranged to count down from a second random number represented by a group of bits of the sequence generated by said pseudo-random number generator (102) and is arranged to load a new value of said second random number and to start again its countdown whenever said first down counter generates its terminal count signal (TC1);

- a recirculating shift register (207), which receives the seeds and feeds said first down counter (205) with said first random number, and which is arranged to generate said randomly rotated version of the seed, in the intervals between the arrivals of two subsequent seeds, by rotating the bits of the seed by an amount determined by the value of said second random number.

3. A random number generator (100) as claimed in claim 1 or 2, characterised in that said pseudo-random generator (102) is a linear feedback shift register, and said alteration signal generator (205, 206, 207) supplies said alteration signal (TC1) to the feedback logic (204b) of said linear feedback shift register.

4. A random number generator (100) as claimed in any preceding claim, characterised in that said mixing logic (103) further comprises an input circuitry (201, 202) arranged to receive the random sequence of bits generated by said true random generator (101), to build said seed by parallelising the bits of said random sequence and to generate a signal (Data Valid) indicating the availability of a seed.

5. A random number generator (100) as claimed in any of claims 2 to 4, characterised in that said recirculating shift register (207) is arranged to load a seed directly, whenever it receives said signal (Data Valid) indicating the availability of the seed, and said pseudo-random generator (102) is arranged to load a new seed upon command of said first counter (205), whenever the latter receives said signal (Data Valid) indicating the availability of the seed.

6. A random number generator (100) as claimed in any preceding claim, characterised in that said input circuitry (201, 202) comprises a clock signal generator (203) for generating, starting from a first clock signal (CLK) timing the operations of said input circuitry (201, 202), a second clock signal, for timing said pseudo-random generator (102) and said alteration signal generator (205, 206, 207), whereby the output bit rate of the random number generator (100) is independent from the rate of the random sequence of bits supplied by the true random generator (101).

7. A random number generator (100) as claimed in any preceding claim, characterised in that it further comprises an output logic (104) for parallelising the altered pseudo-random sequence and building words of a given length, said output logic (104) comprising a scrambler (211) for scrambling the bits in each word in random manner.

8. A random number generator (100) as claimed in claim 7, characterised in that said scrambler (211) is controlled by a random selection signal (SEL) provided by said generator (205, 206, 207) of the alteration signal.

9. A random number generator (100) as claimed in claims 2 and 8, characterised in that said random selection signal is supplied by said recirculating shift register (207).

10. A random number generator as claimed in any of claims 7 to 9, characterised in that said scrambler circuit (211) comprises a switching matrix (301) composed by an n-level binary tree of switches (400), each controlled by a respective bit of said random selection signal so as to scramble or to let through unchanged its input bits.

11. A random number generator as claimed in any of claims 7 to 9, characterised in that it is implemented as an integrated circuit.

12. A method of generation of random numbers, in which said random numbers are generated by altering a pseudo-random sequence by means of true random numbers forming random seeds for the generation of said pseudo-random sequence, the method being characterised in that it comprises the steps of:

- obtaining the random seeds from a random sequence of bits having variable rate;
- processing a random seed to generate an alteration signal (TC1) exploiting the random arrival time of the bits of said sequence of bits; and
- changing the pseudo-random sequence by said alteration signal (TC1) at random instants between the arrival of two subsequent seeds, thereby obtaining in said interval multiple pseudo-random sequences of random lengths shorter than the lengths determined by the arrival of two subsequent seeds, said alteration signal (TC1) being generated under the control of the pseudo-random sequence.

13. A method as claimed in claim 12, characterised in that said alteration signal (TC1) is generated at the end of a first countdown starting from a first random number represented by a randomly variable group of bits that are part of a rotated version of a received seed obtained by rotating the seed by an amount indicated by a second random number represented by a group of bits of the pseudo-random sequence, the first countdown starting whenever a seed is generated and restarting, between the arrival of two subsequent bits, whenever the countdown itself ends; and in that said second random number is the starting value of a second countdown starting whenever the first down counting ends, the end of said second countdown stopping said seed rotation.

14. A method as claimed in claim 12 or 13, characterised in that said pseudo-random sequence is generated by a linear feedback shift register (102), and said alteration signal (TC1) is fed to the feedback logic (204b) of said linear feedback shift register (102).

15. A method as claimed in any of claims 12 to 14, in which the altered pseudo-random sequence is parallelised to create words of a desired length (MAX_COUNT), characterised in that the method further comprises a random scrambling of said words.

16. A method as claimed in claim 15, characterised in that said scrambling is controlled by a random selection signal obtained from the bits used to form said first random number.

17. A method as claimed in any of claims 11 to 14, characterised in that it further comprises the step of generating, starting from a first clock signal timing the seed generation, a second clock signal, for timing the generation of said pseudo-random sequence and of said alteration signal (TC1), the parallelisation of the output words and the scrambling, whereby an output bit rate independent from the rate of the random sequence of bits is obtained.

18. A computer program product loadable in the memory of at least one computer and including software code portions for performing the method of any of claims 12 to 17.